Über die Struktur kommutativer Hauptidealringe

Von G. POLLÁK in Szeged

Herrn Professor László Rédei zum 60. Geburtstag gewidmet

In der vorliegenden Arbeit wird der Begriff „Hauptidealring" im weitesten Sinne benutzt, d. h. es wird weder Nullteilerfreiheit, noch Existenz eines Einselements erfordert. Wir wollen zuerst die Struktur der kommutativen Hauptidealringe mit Einselement (kurz: k. H. E.) untersuchen und dann das bekommene Resultat zur Betrachtung kommutativer Hauptidealringe im allgemeinen zu Hilfe nehmen.

1. Wir nennen π ein *schwaches Primelement*, falls aus $\pi = \alpha\beta$, $\alpha \notin (\pi)$ folgt: $\beta \in (\pi)$. Wir zeigen vor allem:

Hilfssatz 1. *Es sei R ein k. H. E., $\pi \in R$ ein schwaches Primelement und $\mathfrak{v}_{\pi^m}$ der Annihilator*[1]) *von π^m. Ist $\pi^m \neq 0$, $\mathfrak{v}_{\pi^m} \subseteq (\pi)$, so ist (π^m) ein direkter Summand in R.*

Es genügt zu zeigen, daß (π^m) durch einen von 0 verschiedenen Idempotenten erzeugt ist. Zu diesem Zwecke sei $\mathfrak{v}_{\pi^m} = (\alpha)$, $\alpha \notin (\pi)$ und

$$(\alpha, \pi) = (\beta), \quad \beta = \alpha\xi + \pi\eta \quad (\notin (\pi)).$$

Hieraus erhalten wir $\pi = \beta\gamma$. Wegen $\beta \notin (\pi)$ muß $\gamma \in (\pi)$, $\gamma = \pi\gamma'$ sein und

$$\pi^m = \pi^{m-1}\beta\gamma = \pi^m\beta\gamma' = (\alpha\xi + \pi\eta)\pi^m\gamma' = \pi^{m+1}\eta\gamma'.$$

Dann ist aber $\varepsilon = (\pi\eta\gamma')^m$ ein Idempotent und wegen $\pi^m = \pi^m\varepsilon$ ist $(\pi^m) = (\varepsilon)$, $\varepsilon \neq 0$ falls $\pi^m \neq 0$, was zu beweisen war.

Das Hauptresultat in der angedeuteten Richtung ist im folgenden Satz enthalten:

Satz 1. *Jeder k. H. E. R läßt sich in die direkte Summe von endlich vielen solchen unzerlegbaren k. H. E. zerlegen, in denen die eindeutige Primzerlegung gilt.*

---

[1]) Wir wollen statt Annullatorenideal diesen kürzeren Ausdruck benutzen.

Beweis. Wir nehmen an, daß in R die eindeutige Primzerlegung nicht gilt und zeigen, daß R dann in eine direkte Summe von zwei Komponenten zerfällt.

In der Tat, wenn es in R ein schwaches Primelement $\pi \neq 0$ gibt, das nicht prim ist, so sei α ein Nullteiler mod π. Wir können voraussetzen, daß $(\alpha) \supset (\pi)$, denn wir dürfen α durch das Erzeugende α' des Ideals (α, π) ersetzen. In der Tat, wenn $\alpha\beta \in (\pi)$ ist, so gilt auch $\alpha'\beta \in (\alpha\beta, \pi\beta) \subseteq (\pi)$. Dann ist $\pi = \alpha\gamma$, wobei wegen der schwachen Primeigenschaft von π die Gleichung $\gamma = \delta\pi$ mit passendem δ bestehen muß. Hieraus erhalten wir $(1-\alpha\delta)\pi = 0$. Da α offenbar keine Einheit sein kann, ist $1-\alpha\delta \notin (\alpha)$, also wegen $(\alpha) \supset (\pi)$ um so mehr $1-\alpha\delta \notin (\pi)$. Nach Hilfssatz 1 zerfällt dann R in eine direkte Summe, d. h. ist unsere Behauptung in diesem Falle richtig.

Es sei jetzt in R jedes schwache Primelement prim. Ist dann $\alpha \in R$ nicht prim, so gilt mit passenden β, γ

$$\alpha = \beta\gamma, \quad (\beta) \supset (\alpha), \quad (\gamma) \supset (\alpha).$$

Ist einer der Faktoren noch immer nicht prim, so kann man ihn wieder ähnlicherweise zerlegen usw. Da ein Hauptidealring immer die Maximumbedingung (für Ideale) erfüllt, führt dieser Zerlegungsprozeß in endlich vielen Schritten zu einer Primzerlegung. Damit gibt es für jedes Element von R wenigstens eine Primzerlegung, und nach unserer Annahme gibt es für irgendwelches $\alpha \neq 0$ zwei wesentlich (d. h. nicht nur in Ordnung und Einheitsfaktoren) verschiedene Zerlegungen:

$$\alpha = \pi_1^{i_1} \dots \pi_n^{i_n} = \varepsilon \pi_1^{j_1} \dots \pi_n^{j_n}, \tag{1}$$

wobei ε eine Einheit ist; aus $\varepsilon' \pi_s = \pi_t$ mit irgendwelcher Einheit ε' folgt $s = t$; $i_s, j_s \geqq 0$, $i_s + j_s > 0$ für alle $1 \leqq s \leqq n$; für irgendwelches s gilt $i_s \neq j_s$. Wir unterscheiden zwei Fälle.

a) Nicht alle i und j sind von 0 verschieden. Sei z. B. $j_1 = 0$. Da π_1 ein Primelement ist, muß einer der Faktoren auf der rechten Seite von (1) (z. B. π_2) in (π_1) enthalten sein, d. h.

$$\pi_2 = \pi_1 \varrho. \tag{2}$$

Wir haben erhalten, daß das Primelement π_2 reduzibel ist, d. h. es läßt sich in zwei Faktoren zerlegen, aus denen keiner eine Einheit ist (von der Primeigenschaft von π_1 werden wir im Folgenden schon keinen Nutzen machen). Aus (2) folgt, daß entweder $\pi_1 \in (\pi_2)$ oder $\varrho \in (\pi_2)$. Sei z. B. $\varrho = \sigma\pi_2$. Daraus und aus (2) ergibt sich

$$(1-\pi_1\sigma)\pi_2 = 0.$$

Da wegen (2) $(\pi_2) \subset (\pi_1) \neq (1)$, ist $1-\pi_1\sigma \notin (\pi_2)$, der Annihilator von π_2

ist also nicht in (π_2) enthalten. Damit ist (π_2) nach Hilfssatz 1 ein direkter Summand in R.

b) Alle i und j sind in (1) von 0 verschieden. Es gibt ein s, für welches $i_s \neq j_s$ ist; bestimmtheitshalber sei $0 < i_1 < j_1$. Wir setzen $\pi_2^{i_2} \dots \pi_n^{i_n} = \beta$, $\varepsilon \pi_1^{j_1 - i_1} \pi_2^{i_2} \dots \pi_n^{i_n} = \gamma$. Dann haben wir

$$(\beta - \gamma)\pi_1^{i_1} = 0.$$

Wäre hier $\beta - \gamma \in (\pi_1)$, so wäre auch $\beta \in (\pi_1)$ und wir hätten

$$\beta = \pi_2^{i_2} \dots \pi_n^{i_n} = \pi_1 \beta',$$

d. h. wieder Fall a). Ist dagegen $\beta - \gamma \notin (\pi_1)$, so ist der Annihilator von $\pi_1^{i_1}$ nicht in (π_1) enthalten, also ist in diesem Falle wieder $(\pi_1^{i_1})$ ein direkter Summand in R.

Es gilt also $R = R_{11} \dotplus R_{12}$. Als direkte Summanden eines Ringes mit Einselement, sind R_{11} und R_{12} auch solche Ringe. Ferner sind R_{11} und R_{12} Hauptidealringe, denn wenn $\mathfrak{a}$ ein Ideal z. B. in R_{11} ist, so ist es auch in R ein Ideal, und wenn $\mathfrak{a} = (\alpha)$ in R, so besteht dasselbe auch in R_{11}. Endlich, wenn wir diesen Zerlegungsprozeß fortsetzen, muß dieser nach endlich vielen Schritten abbrechen. Um das zu zeigen, betrachten wir einen Ring R der unbegrenzt zerlegbar ist, d. h. für welchen die unendlich vielen Zerlegungen

$$\begin{aligned} &R = R_{11} \dotplus R_{12}, \\ &R = R_{21} \dotplus R_{22} \dotplus R_{23}, \\ &\dots\dots\dots\dots\dots\dots \\ &R = R_{n1} \dotplus \dots \dotplus R_{n,n+1}, \\ &\dots\dots\dots\dots\dots\dots \end{aligned} \qquad (R_{ij} \neq 0 \text{ für } i = 1, 2, \dots; \; j = 1, \dots, i+1) \tag{3}$$

gelten, wo die n-te Zerlegung aus der $(n-1)$-ten so entsteht, daß eine der Komponenten in zwei nichttriviale Summanden zerlegt wird. Es ist klar, daß in jeder Zerlegung wenigstens eine Komponente auch selbst unbegrenzt zerlegbar ist; darum können wir ohne Beschränkung der Allgemeinheit annehmen, daß in jeder Zerlegung in (3) immer die letzte Komponente zerlegbar ist und

$$R_{n-1,1} = R_{n1}, \dots, R_{n-1,n-1} = R_{nn-1}; \quad R_{n-1,n} = R_{nn} \dotplus R_{nn+1}$$

gilt. Dann ist aber

$$R_{11} \subset R_{11} \dotplus R_{22} \subset \dots \subset R_{11} \dotplus R_{nn} \subset \dots$$

eine unendliche aufsteigende Idealkette. Das ist aber wegen der Maximumbedingung unmöglich. Damit ist Satz 1 bewiesen.

Es ist leicht zu sehen, daß die direkte Summe R von endlich vielen Hauptidealringen mit Einselement $R_1, \dots, R_k$ wieder ein Hauptidealring mit

Einselement ist. In der Tat, ein Ideal $\mathfrak{a}$ in R ist eine direkte Summe von gewissen Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ in $R_1, \ldots, R_k$. Ist dabei $\mathfrak{a}_i = (a_i)$ in R_i für jedes $1 \leqq i \leqq k$, so haben wir

$$\mathfrak{a} = \mathfrak{a}_1 \dotplus \cdots \dotplus \mathfrak{a}_k = (a_1) \dotplus \cdots \dotplus (a_k) = (a_1 + \cdots + a_k).$$

Durch diese Bemerkung und Satz 1 ist die Frage über sämtliche k. H. E. auf die Frage über direkt unzerlegbare k. H. E. (kurz: u. H. E.) zurückgeführt. Aus Satz 1 folgt unmittelbar, daß in einem u. H. E. die eindeutige Primzerlegung immer gilt. Um alle solche Ringe angeben zu können, brauchen wir zwei Hilfssätze.

Hilfssatz 2. *Sei R ein k. H. E., (π) ein Primideal darin und $(\varrho) \supset (\pi)$. Dann ist*

$$(\varrho\,\pi) = (\pi). \tag{4}$$

In der Tat, wegen $(\varrho) \supset (\pi)$ haben wir

$$\pi = \varrho\,\pi'.$$

Aus der Primeigenschaft von π folgt aber $\pi' \in (\pi)$, also $\pi \in (\varrho\,\pi)$ und damit auch (4).

Hilfssatz 3. *Gilt in einem k. H. E. R für das Primideal (π)*

$$(\pi) \supset (\pi^2) \supset \cdots, \tag{5}$$

so ist das Ideal

$$(\sigma) = \bigcap_{i=1}^{\infty} (\pi^i) \tag{6}$$

prim in R.

Wäre nämlich $\alpha\beta \in (\sigma)$ und

$$\alpha = \alpha'\pi^k, \quad \beta = \beta'\pi^l \qquad (\alpha', \beta' \notin (\pi);\ k, l \geqq 0),$$

wobei $k = 0$ oder $l = 0$ bedeutet, daß $\alpha \notin (\pi)$ bzw. $\beta \notin (\pi)$, so hätten wir $\alpha'\beta' \notin (\pi)$, aber wegen (6) ist

$$\alpha'\beta'\pi^{k+l} \in (\pi^{k+l+1}). \tag{7}$$

Sei $(\alpha'\beta', \pi) = (\varrho)$; dann ist $(\pi) \subset (\varrho)$, also nach Hilfssatz 2 besteht auch (4). Aus (7) folgt aber

$$(\varrho\,\pi^{k+l}) \subseteq (\pi^{k+l+1}).$$

Mit (4) zusammen ergibt dies

$$(\pi^{k+l}) = (\pi^{k+l+1}),$$

was aber mit (5) in Widerspruch steht.

Nun können wir beweisen den

Satz 2. *Ein u. H. E. ist entweder nullteilerfrei oder hat ein einziges, und zwar nilpotentes Primideal.*

Beweis. Sei R ein u. H. E. Wir bemerken vor allem, daß in R jedes von (0) verschiedene Primideal maximal ist. In der Tat, nach Satz 1 gilt in R die eindeutige Primzerlegung. Wäre nun das Primideal $(\pi) \neq (0)$ nicht maximal, so wäre es in einem maximalen, also primen Ideal (ϱ) enthalten. Nach Hilfssatz 2 gilt dann aber (4), also $\pi = \pi\varrho\xi$, in Widerspruch mit der Eindeutigkeit der Primzerlegung.

Es sei jetzt (π) ein Primideal in R. Gilt für ihn (5), so ist nach Hilfssatz 3 das durch (6) definierte Ideal (σ) prim, also wegen $(\pi) \supset (\sigma)$ muß $\sigma = 0$ sein. Wir haben erhalten, daß wenn in R für irgendwelches Primideal (5) gilt, so ist in R das Ideal (0) prim, d. h. R ist nullteilerfrei (und damit gilt natürlich (5) für alle Primideale).

Gilt (5) für ein Primideal (π) nicht (also gilt es für kein Primideal), so ist $(\pi^m) = (\pi^{m+1})$ für passendes m, d. h. $\pi^m = \pi^{m+1}\xi$. Wegen der Eindeutigkeit der Primzerlegung in R folgt daher $\pi^m = 0$, d. h. alle Primideale von R sind nilpotent. Wäre nun (τ) ein von (π) verschiedenes Primideal, so wäre auch (τ, π) nilpotent; aus der Maximalität von (τ) und (π) folgt aber $(\tau, \pi) = (1)$: Wiederspruch. In diesem Falle hat also R ein einziges Primideal (π). Damit ist Satz 2 bewiesen.

Jetzt steht die Struktur der k. H. E. schon ganz klar vor uns. Ein solcher Ring ist eine direkte Summe von endlich vielen „Hauptidealintegritätsbereichen" (Typ I) und Ringen mit einem einzigen (maximalen) nilpotenten Primideal (Typ II). Ringe beider Typen I und II sind direkt unzerlegbar, jedes Primideal in ihnen ist maximal und damit gilt in ihnen die Eindeutigkeit der Primzerlegung. Umgekehrt, eine direkte Summe von endlich vielen Ringen vom Typ I und II ist immer ein k. H. E.

Es ist leicht zu sehen, daß die Eindeutigkeit der Primzerlegung nur im unzerlegbaren Falle gilt. Ein direkt zerlegbarer k. H. E. enthält nämlich einen von 0 und Einheiten verschiedenen Idempotenten, dessen Primzerlegung nicht eindeutig ist. Wenn wir aber — statt die Eindeutigkeit im strengen Sinne (d. h. im Sinne, daß in (1) $i_m = j_m$ für jedes m) zu erfordern — nur $\pi_m^{i_m} = \varepsilon_m \pi_m^{j_m}$ mit einer Einheit ε_m voraussetzen, so erhalten wir, daß *die Ringe, in denen die Primzerlegung in diesem schwächeren Sinne eindeutig ist, entweder zu dem Typ I gehören oder eine direkte Summe von endlich vielen Körpern und Ringen vom Typ II sind und umgekehrt, alle solche Ringe erfüllen diese Forderung.* Um die erste Behauptung einzusehen, müssen wir zeigen, daß in einem k. H. E., in welcher die Primzerlegung im schwächeren Sinne ein-

deutig ist, jeder nichttriviale direkte Summand ersten Types ein Körper ist. Wäre nun $R = R_1 \dotplus R_2$, wobei R_1 nullteilerfrei, aber kein Körper ist, so wäre R_2 ein Primideal in R, aber nicht maximal. Nach Hilfssatz 2 gilt dann für $R_2 = (\pi)$ (4) und damit ist π mehrdeutig zerlegbar, also muß $\pi = 0$ und damit $R_2 = 0$ gelten. Umgekehrt, wenn

$$R = K_1 \dotplus \cdots \dotplus K_l \dotplus N_1 \dotplus \cdots \dotplus N_m$$

ist, wo die K_i Körper, die N_j Ringe vom Typ II sind, so sind

$$\mathfrak{p}_i = K_1 \dotplus \cdots \dotplus K_{i-1} \dotplus K_{i+1} \dotplus \cdots \dotplus K_l \dotplus N_1 \dotplus \cdots \dotplus N_m \qquad (i = 1, \ldots, l),$$

$$\mathfrak{p}_{l+j} = K_1 \dotplus \cdots \dotplus K_l \dotplus N_1 \dotplus \cdots \dotplus N_{j-1} \dotplus \mathfrak{q}_j \dotplus N_{j+1} \dotplus \cdots \dotplus N_m \qquad (j = 1, \ldots, m)$$

die sämtlichen Primideale von R; hier bedeutet $\mathfrak{q}_j$ das Primideal von N_j. Sie sind alle maximal (die Faktorringe sind Körper)[2]). Daraus folgt unmittelbar, daß Elemente, die dasselbe Primideal erzeugen, assoziiert sein müssen. Folglich erzeugen in (1) $\pi_1, \ldots, \pi_n$ voneinander verschiedene Primideale. Sind nun z. B. $\pi_s^{i_s}$ und $\pi_s^{j_s}$ nicht assoziiert und ist $(\pi_s) = \mathfrak{p}_k$, so kann (1) nicht bestehen, denn die Komponenten aus K_k (falls $k \leqq l$) bzw. N_{k-l} (falls $k > l$) auf beiden Seiten verschieden sind.

Im allgemeinen Falle gibt es eine in gewissem Sinne minimale Zerlegung, die schon eindeutig bestimmt ist. Sei nämlich $R = R_1 \dotplus \cdots \dotplus R_m$, wo alle R_i u. H. E. sind. Sämtliche Primideale von R entstehen jetzt in der Form

$$\mathfrak{p} = R_1 \dotplus \cdots \dotplus R_{i-1} \dotplus \bar{\mathfrak{p}} \dotplus R_{i+1} \dotplus \cdots \dotplus R_m \qquad (1 \leqq i \leqq m),$$

wo $\bar{\mathfrak{p}}$ ein Primideal in R_i (möglicherweise auch (0)) ist. Es ist klar, daß $\mathfrak{p}$ durch das Element $\pi = \varepsilon_1 + \cdots + \varepsilon_{i-1} + \bar{\pi} + \varepsilon_{i+1} + \cdots + \varepsilon_m$ erzeugt ist, wobei ε_j der in R_j enthaltene Idempotent, $\bar{\pi}$ ein fixiertes Erzeugende von $\bar{\mathfrak{p}}$ ist. *Für jedes Element $a \neq 0$ von R gibt es eine einzige Darstellung in der Form eines Produktes von solchen π*

$$a = \varepsilon \pi_1^{i_1} \ldots \pi_n^{i_n} \qquad (\varepsilon \text{ Einheit}, \ i_s > 0)$$

mit der Eigenschaft, daß aus $a = \varepsilon' \pi_1^{j_1} \ldots \pi_n^{j_n}$, wo ε' eine Einheit und $j_s \geqq 0$ ist, $i_s \leqq j_s$ für $s = 1, \ldots, n$ folgt. Den Beweis überlassen wir dem Leser.

2. Es sei jetzt R ein beliebiger kommutativer Hauptidealring. Nach J. SZENDREI nennen wir das Element $r \in R$ einen *Multiplikator*, falls es eine natürliche Zahl n mit

$$r\xi = n\xi \quad \text{für alle} \quad \xi \in R \tag{8}$$

gibt. Es bezeichne ferner N den Zeroring mit einem unendlich zyklischen

[2]) Wir sehen also, daß die schwächere Eindeutigkeit gleichbedeutend mit der Maximalität sämtlicher Primideale ist.

Modul. Es ist klar, daß N ein kommutativer Hauptidealring ist. Außerdem gilt

Satz 3. *Enthält der kommutative Hauptidealring R keinen Multiplikator, so ist*

$$R \cong R_1 \dotplus N, \tag{9}$$

wobei R_1 entweder 0 oder ein k. H. E. ist.

Beweis. Es sei $R=(\alpha)$. Ein Element ν ist dann und nur dann ein Multiplikator, falls $\nu\alpha = n\alpha$ mit einer natürlichen Zahl n besteht. Daraus folgt, daß $\varrho\alpha + r\alpha = \sigma\alpha + s\alpha$ nur im Fall $r=s$ gelten kann.

Betrachten wir das Ideal $\mathfrak{a}=(p\alpha, \alpha^2)$ mit einer beliebigen Primzahl p. Jedes Element von $\mathfrak{a}$ entsteht in der Form $\xi\alpha + xp\alpha$ ($\xi \in R$) und da $\mathfrak{a}$ ein Hauptideal ist, ist es durch ein solches Element, z. B. durch $\varkappa = \varrho\alpha + rp\alpha$ erzeugt. Es gilt also

$$p\alpha = \sigma\varkappa + s\varkappa = (\sigma\varrho + s\varrho + rp\sigma)\alpha + srp\alpha, \tag{10}$$

$$\alpha^2 = \tau\varkappa + t\varkappa = (\tau\varrho + t\varrho + rp\tau)\alpha + trp\alpha, \tag{11}$$

also aus (10) $srp = p$, $s = r = \pm 1$ und aus (11) $trp = 0$, $t = 0$. Wir können jetzt (11) in der Form $\alpha^2 = \tau\varrho\alpha + p\tau\alpha$ schreiben. Setzen wir $\tau = \zeta\alpha + z\alpha$, so erhalten wir hieraus $\xi\alpha^2 + (zp-1)\alpha^2 = 0$ mit irgendwelchem $\xi \in R$, d. h. $\xi\alpha + (zp-1)\alpha$ ist ein Annullator von α und damit auch des ganzen Ringes R. Sei nun $\mathfrak{o}=(\omega)$ der Annihilator von R und sei $\omega \equiv o\alpha \bmod \alpha^2$. Wegen $\xi\alpha + (zp-1)\alpha \in (\omega)$ ist $\omega \neq 0$. Da ferner $m\omega$ ($m = 0, \pm 1, \ldots$) die sämtlichen Elemente von (ω) sind, ist sogar $o \neq 0$, denn aus $m\omega = \xi\alpha + (zp-1)\alpha$ auch $mo = zp - 1 \equiv -1 \bmod p$ folgt. Aus dem letzten schließen wir sogar $p \nmid o$. Da hier p eine beliebige Primzahl ist, muß $o = \pm 1$ sein, also wegen $m\omega \equiv mo\alpha \bmod \alpha^2$ ist einerseits $(\omega) \cap (\alpha^2) = 0$, andererseits $(\omega, \alpha^2) = R$, d. h.

$$R = (\alpha^2) \dotplus (\omega).$$

Hier ist $(\omega) \cong N$. Als direkter Summand von einem Hauptidealring, ist (α^2) selber ein solcher. Es bleibt also übrig zu zeigen, daß entweder $\alpha^2 = 0$ ist oder (α^2) ein Einselement hat. Wir haben schon gesehen, daß $\omega = \lambda\alpha \pm \alpha$ mit einem $\lambda \in R$ ist. Ohne Beschränkung der Allgemeinheit können wir $\omega = \lambda\alpha - \alpha$ setzen. Aus $\omega\alpha = 0$ folgt dann $\lambda\alpha^2 = \alpha^2$ und auch

$$\lambda^2\alpha^2 = \alpha^2, \tag{12}$$

also falls $\alpha^2 \neq 0$, so ist auch $\lambda^2 \neq 0$. Da ferner $\lambda^2 \in (\alpha^2)$ ist, so bedeutet (12), daß in diesem Falle λ^2 das Einselement von (α^2) ist. Dies vollendet den Beweis des Satzes 3.

Es ist leicht zu sehen, daß auch umgekehrt, jeder Ring von der Form

(9) ein kommutativer Hauptidealring ohne Multiplikator ist. In der Tat, es sei $\mathfrak{a}$ ein Ideal von R. Ist $R_1 = 0$, so ist offenbar $\mathfrak{a} = (m\omega)$ mit einer ganzen Zahl m und mit demjenigen ω, das R erzeugt. Ist dagegen $R_1 \neq 0$, also R ein k. H. E., so ist

$$R = (\omega) \dotplus (\varepsilon),$$

wo ε ein Idempotent, ω ein Annullator von R ist. Dann gilt

$$\mathfrak{a} = (a\omega) \dotplus (\alpha) = (a\omega + \alpha). \tag{13}$$

Die erste Hälfte von (13) folgt aus der allgemeinen Tatsache, daß in einem Ringe R mit $R = R_1 \dotplus R_2$, wo R_1 ein Ring mit Einselement ist, jedes Ideal $\mathfrak{a}$ sich in der Form $\mathfrak{a} = \mathfrak{a}_1 \dotplus \mathfrak{a}_2$ darstellen läßt, wobei $\mathfrak{a}_i$ $(i = 1, 2)$ ein Ideal von R_i ist. Die zweite Gleichung folgt daraus, daß $\varepsilon(a\omega + \alpha) = \alpha$, d. h. $\alpha \in (a\omega + \alpha)$, $a\omega \in (a\omega + \alpha)$ und folglich $\mathfrak{a} \subseteq (a\omega + \alpha)$ ist. Endlich, wegen $r\omega = 0$ $(r \in R)$, $n\omega \neq 0$ $(n = 1, 2, \ldots)$ enthält R keinen Multiplikator. Unsere Behauptung ist damit bewiesen.

Damit haben wir eine Übersicht von den kommutativen Hauptidealringen ohne Multiplikator bekommen. Bezüglich der übriggebliebenen kommutativen Hauptidealringe beweisen wir

Satz 4. *Ein kommutativer Hauptidealring R hat dann und nur dann eine Schreiersche k. H. E.-Erweiterung R^** (d. h. eine Schreiersche Erweiterung R^*, die ein k. H. E. ist), *wenn R einen Multiplikator enthält. In diesem Falle gibt es sogar einen R^* mit $R^*/R \cong I/(n)$, wo I der Ring der ganzen rationalen Zahlen und $n \neq 0$ ist.*

Beweis. Enthält R keinen Multiplikator, so sei (ω) der Annihilator von R. Nach Satz 3 ist (ω) ein von (0) verschiedener direkter Summand von R. Wäre nun R^* eine Schreiersche k. H. E.-Erweiterung von R, so wäre (ω) ein Ideal auch in R^*[3]). Ist $R^* = R_1^* \dotplus \cdots \dotplus R_n^*$, wo jeder Summand ein u. H. E. ist, so ist (ω) in einem R_i^* enthalten, denn (ω) offenbar direkt unzerlegbar ist. Dann gehört R_i^* zum Typ II, denn wegen $\omega^2 = 0$ R_i^* nicht nullteilerfrei sein kann. Bezeichnet $\mathfrak{p}_i$ das Primideal von R_i^* und ist $\mathfrak{p}_i^n = 0$, $\mathfrak{p}_i^{n-1} \neq 0$, so ist es leicht zu sehen, daß $\mathfrak{p}_i^{n-1} = (\omega)$ sein muß. Da ferner $(\mathfrak{p}_i^{n-1})^+ \cong \cong (R_i^*/\mathfrak{p}_i)^+$ ist, muß $R_i^*/\mathfrak{p}_i$ ein Körper mit einem unendlich zyklischen Modul sein. Einen solchen gibt es aber nicht. Dieser Widerspruch vollendet den Beweis der Notwendigkeit.

Sei jetzt $r \in R$ ein Multiplikator, für den (8) gilt, und zwar nehmen wir an, daß n die kleinste natürliche Zahl ist, für die (8) mit passendem $r \in R$ besteht (d. h. n ist ein Teiler von allen solchen Zahlen). Es sei ferner $R = (\alpha)$.

[3]) Siehe [1], Satz 2.

Dann ist offenbar $R/(\alpha^2)$ ein Zeroring mit zyklischem Modul von Ordnung n. Zuerst betrachten wir den Fall, daß der Annihilator von R $\mathfrak{o}=(\omega)\neq(0)$ ist. Wegen

$$n\omega=\nu\omega=0$$

sind dann $\omega,\ldots,(m-1)\omega$, $m\omega=0$ $(m|n)$ sämtliche verschiedene Elemente von $\mathfrak{o}$. Endlich sei

$$\nu\equiv n_1\alpha,\quad \omega\equiv o_1\alpha \mod \alpha^2 \qquad (0\leqq n_1, o_1<n). \tag{14}$$

Ist dabei $o_1\neq(0)$, so können wir ω so wählen, daß

$$o_1|n \tag{15}$$

ist. In der Tat, sei ω^* ein beliebiges Erzeugende von $\mathfrak{o}$ und sei $\omega^*\equiv o^*\alpha \mod \alpha^2$. Es ist klar, daß auch $c\omega^*$ ein Erzeugende von $\mathfrak{o}$ ist, falls $(c, n)=1$ besteht. Wir können jetzt c so wählen, daß $co^*\equiv(o^*, n) \mod n$ gilt. Aus der letzten Kongruenz folgt aber $c\omega^*\equiv(o^*, n)\alpha \mod \alpha^2$, so daß (15) mit $\omega=c\omega^*$, $o_1=(o^*, n)$ erfüllt ist. Wir können sogar erreichen, daß

$$(n_1, n)|o_1 \tag{16}$$

gelte. Zu diesem Zwecke bemerken wir, daß sämtliche verschiedene Elemente von R, für die (8) gilt, $\nu+k\omega$ $(k=0, 1,\ldots,m-1)$ sind. Aus (14) folgt

$$\nu+k\omega\equiv(n_1+ko_1)\alpha \mod \alpha^2.$$

Für ein passendes k gilt dabei (16) für n_1+ko_1 statt n_1[4]); wir dürfen annehmen, daß dies schon für $k=0$ der Fall ist. Damit haben wir auch ν festgesetzt.

Jetzt konstruieren wir einen Erweiterungsring mit Einselement R^* von R folgendermaßen. Sämtliche verschiedene Elemente von R^* seien $\varrho+r$ $(\varrho\in R, r$ ganze Zahl, $0\leqq r<n)$. Die Verknüpfungen in R^* definieren wir durch

$$\begin{aligned}(\varrho+r)+(\sigma+s)&=\left(\varrho+\sigma+\left[\frac{r+s}{n}\right]\nu\right)+\left(r+s-\left[\frac{r+s}{n}\right]n\right),\\ (\varrho+r)(\sigma+s)&=\left(\varrho\sigma+s\varrho+r\sigma+\left[\frac{rs}{n}\right]\nu\right)+\left(rs-\left[\frac{rs}{n}\right]n\right).\end{aligned} \tag{17}$$

Es ist klar, daß R^* ein Ring ist, die Elemente $\varrho+0$ (die wir im folgenden mit ϱ identifizieren werden) bilden in R^* ein mit R isomorphes Ideal, das durch α erzeugt ist und wofür $R^*/\alpha\cong I/(n)$ gilt. Ferner ist das Element $0+1$ (im folgenden durch 1 bezeichnet, sowie die Elemente $0+r$ durch r) das

[4]) Es ist leicht zu sehen, daß es zu jedem Triplet von ganzen rationalen Zahlen a, b, c ein x gibt, so daß $(a+xc, b)|c$ gilt.

Einselement in R^*[5]). Bemerken wir noch, daß jedes Ideal (ϱ) von R auch Ideal von R^* ist, und durch dasselbe ϱ erzeugt wird, ist also ein Hauptideal auch in R^*. Endlich, der Annihilator von (α) in R^* ist wieder gleich (ω). Wir wollen zeigen, daß R^* ein Hauptidealring ist.

Bemerken wir vor allem, daß in R^* jedes Ideal $\mathfrak{a}$ durch höchstens zwei Elemente erzeugbar ist. Aus dem ersten Isomorphiesatz erhalten wir nämlich

$$\mathfrak{a}/\mathfrak{a}\cap(\alpha)\cong(\mathfrak{a},\alpha)/(\alpha).$$

Die rechte Seite dieses Isomorphismus ist ein Ideal in $R^*/(\alpha)$, ist also isomorph mit einem Unterringe $(d)/(n)$ von $I/(n)$, $d|n$. Daher ist der Ring $\mathfrak{a}/\mathfrak{a}\cap(\alpha)$ durch ein einziges Element erzeugbar, und da wegen $\mathfrak{a}\cap(\alpha)\subseteq(\alpha)$ das Ideal $\mathfrak{a}\cap(\alpha)$ ein Hauptideal ist, ist $\mathfrak{a}$ durch zwei Elemente erzeugbar.

Aus dem Bewiesenen folgt, daß in R^* die Maximumbedingung für Ideale erfüllt ist. Darum genügt es zu zeigen, daß in R^* jedes irreduzible Ideal (d. h. jedes Ideal $\mathfrak{a}$, für welches aus $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$ $\mathfrak{b}=\mathfrak{a}$ oder $\mathfrak{c}=\mathfrak{a}$ folgt) ein Hauptideal ist. Hieraus folgt nämlich die Hauptidealeigenschaft für sämtliche Ideale durch vollständige Induktion. Wir werden also zeigen, daß ein Ideal entweder reduzibel oder ein Hauptideal ist.

Betrachten wir zuerst diejenigen Ideale $\mathfrak{a}$, die α enthalten; sie sind alle in der Form $\mathfrak{a}=(\alpha,d)$ darstellbar, wo $d|n$ ist. Sei $dd'=n$. Das Ideal $(\alpha,d)(\alpha)=(\alpha^2,d\alpha)$ sei durch $\gamma=(\beta+bd)\alpha$ erzeugt. Dann ist erstens $(\eta+y)\gamma=d\alpha$ mit passenden η, y und da $(\eta+y)\gamma\equiv ybd\alpha \bmod \alpha^2$ ist, muß

$$(b,d')=1 \tag{18}$$

gelten. Zweitens, mit passenden ξ, x gilt auch $(\xi+x)\gamma=\alpha^2$, also

$$(\xi+x)(\beta+bd+z\omega)=\alpha+t\omega \tag{19}$$

mit beliebigem z. Hieraus sieht man vor allem $xbd\in(\alpha)$, d. h. $n|xbd$ und wegen (18) $d'|x$. Sei $x=d'x'$, $\xi\equiv x_1\alpha$, $\beta\equiv b_1\alpha \bmod \alpha^2$. Dann gehen wir von (19) zur Kongruenz

$$(xb_1+x_1bd)\alpha+xz\omega+x'by\equiv\alpha+t\omega \qquad \bmod \alpha^2$$

über, woher wir auf Grund von (14)

$$x'(d'(b_1+zo_1)+bn_1)+x_1bd\equiv 1+to_1 \qquad \bmod n \tag{20}$$

bekommen. Wir führen noch die Bezeichnung

$$(d'(b_1+zo_1)+bn_1, bd, n)=d_z$$

ein. Aus (20) folgt

$$(d_z, o_1)=1. \tag{21}$$

[5]) Über die Konstruktion und die nachfolgenden Bemerkungen siehe [1].

Wegen (18) und $d|n$ gilt auch $d_z=(d'(b_1+zo_1)+bn_1, d)$. Wir können jetzt z_0 so wählen, daß $d_{z_0}|d'o_1$ sei (siehe die Fußnote [4]), also wegen (21) $d_{z_0}|d'$. Dann ist aber $d_{z_0}|bn_1$ und wegen (18) $(d_{z_0}, b)=1$, d. h.

$$d_{z_0}|n_1. \tag{22}$$

Da andererseits $d_{z_0}|n$ ist, ergibt sich aus (22), (16) und (21) $d_{z_0}=1$. Einfachheitshalber sei $z_0=0$. Dann ist

$$(\alpha, d)=(\beta+bd). \tag{23}$$

In der Tat, es gilt

$$d'(\beta+bd)\alpha\equiv(d'b_1+bn_1)\alpha \qquad \bmod \alpha^2,$$
$$(\beta+bd)\alpha\equiv bd\alpha \qquad \bmod \alpha^2.$$

Wegen (18) wird mit passendem u auch $u(\beta+bd)\alpha\equiv d\alpha \bmod \alpha^2$. Da aber jetzt $(d'b_1+bn_1, d)=d_0=1$ ist, gibt es in $(\beta+bd)$ ein Element ϱ mit $\varrho\equiv\alpha \bmod \alpha^2$. Hieraus und aus $\alpha^2\in(\beta+bd)$ folgt $\alpha\in(\beta+bd)$ und dann auch $d\in(\beta+bd)$, also $(\alpha, d)\subseteq(\beta+bd)$. Da die umgekehrte Inklusion trivial ist, ist (23) richtig. Damit haben wir bewiesen, daß jedes Ideal $\mathfrak{a}$ mit $\alpha\in\mathfrak{a}$ ein Hauptideal ist.

Nehmen wir jetzt an: $\alpha\notin\mathfrak{a}$. Wir haben schon gesehen, daß $\mathfrak{a}$ durch zwei Elemente erzeugbar ist; aus den dort gesagten sieht man sogar, daß für eines der Erzeugenden ein β gewählt werden kann, wofür $(\beta)=\mathfrak{a}\cap(\alpha)$ gilt. Es durchläufe dabei $\varrho+r$ sämtliche Elemente von $\mathfrak{a}$ und bezeichne d den größten gemeinsamen Teiler der so bekommenen r; dann gibt es natürlich in $\mathfrak{a}$ Elemente $\sigma+sd$ mit $\left(s, \frac{n}{d}\right)=1$ und es ist klar, daß jedes solche Element mit β zusammen schon $\mathfrak{a}$ erzeugt:

$$\mathfrak{a}=(\beta, \sigma+sd).$$

Es sei jetzt $\mathfrak{a}(\alpha)=(\tau)$. Dann ist $\tau=(\xi+x)\beta\alpha+(\eta+y)(\sigma+sd)\alpha$. Hier ist $\tau=ysd\alpha \bmod \alpha^2$ und es ist klar, daß $\left(ys, \frac{n}{d}\right)=1$ gelten muß. Darum erzeugt β auch zusammen mit $\delta+qd=(\xi+x)\beta+(\eta+y)(\sigma+sd)$ dasselbe Ideal $\mathfrak{a}$. Wir haben also:

$$\mathfrak{a}=(\beta, \delta+qd);\quad \mathfrak{a}\cap(\alpha)=(\beta);\ \mathfrak{a}(\alpha)=((\delta+qd)\alpha) \tag{24}$$

und $\left(q, \frac{n}{d}\right)=1$.

Offenbar enthält das Ideal (α, d) unser Ideal $\mathfrak{a}$. Da (α, d) ein Hauptideal ist, gilt mit einem passenden $\mathfrak{b}$ sogar

$$(\alpha, d)\mathfrak{b}=\mathfrak{a}.$$

Wegen $\alpha \notin \mathfrak{a}$ ist $\mathfrak{a} \neq (\alpha, d)$. Es genügt also zu zeigen, daß entweder $\mathfrak{b} \neq \mathfrak{a}$, oder $\mathfrak{a}$ ein Hauptideal ist.

Ist $\left(d, \frac{n}{d}\right) = d_1 \neq 1$, so besteht der erste Fall dieser Alternative. Wäre nämlich $(\alpha, d)\mathfrak{a} = \mathfrak{a}$, so wäre auch $(\alpha^2, d\alpha)\mathfrak{a} = \mathfrak{a}(\alpha)$. Aber es ist

$$(\alpha^2, d\alpha)\mathfrak{a} = (\beta\alpha^2, d\beta\alpha, (\delta + qd)\alpha^2,\ d(\delta + qd)\alpha) \subseteq (\alpha^2, d_1 d\alpha),$$

wo doch $(\delta + qd)\alpha \in \mathfrak{a}(\alpha)$, $(\delta + qd)\alpha \notin (\alpha^2, d_1 d\alpha)$, was unmöglich ist.

Ist $\left(d, \frac{n}{d}\right) = 1$, so sei $\beta = (\gamma + c)\alpha$, $(c, n) = \bar{d}$. Wir unterscheiden zwei Fälle, je nachdem $\bar{d} = d$ gilt oder nicht. Zuerst bestehe der zweite Fall; wegen (24) gilt jedenfalls $\bar{d} | d$. Wir zeigen, daß wieder $\mathfrak{b} \neq \mathfrak{a}$ ist. Wäre nämlich $(\alpha, d)\mathfrak{a} = \mathfrak{a}$, so wäre auch

$$(25) \qquad (\beta) = \mathfrak{a} \cap (\alpha) = (\alpha, d)\mathfrak{a} \cap (\alpha) = (d\beta, (\delta + qd)\alpha, d(\delta + qd)) \cap (\alpha).$$

Jedes Element der rechten Seite, u. a. auch β, läßt sich in der Form

$$\beta = d(\xi + x)\beta + (\eta + y)(\delta + qd)\alpha + d(\zeta + z)(\delta + qd) \qquad (zqd^2 \in (\alpha))$$

darstellen. Aber $zqd^2 \in (\alpha)$ ist gleichbedeutend mit $n | zqd^2$, d. h. $\frac{n}{d} \Big| zqd$. Wegen $\left(qd, \frac{n}{d}\right) = 1$ folgt hieraus $\frac{n}{d} \Big| z$; dann ist aber schon $zqd \in (\alpha)$ und damit $\beta \in (\alpha^2, d\alpha)$, im Widerspruch mit der Annahme $\bar{d} \neq d$.

Nun betrachten wir den Fall $\left(d, \frac{n}{d}\right) = 1$, $\bar{d} = d$. Dann gilt

$$(\alpha, d)(\gamma + c + z\omega, \delta + qd) = (\alpha, \delta + qd)(\gamma + c + z\omega, \delta + qd) =$$
$$= (\beta, c(\delta + qd), qd(\delta + qd)) = \mathfrak{a},$$

das letzte wegen $\left(c, qd, \frac{n}{d}\right) = 1$ und wegen der Gleichung

$$(\beta, c(\delta + qd), qd(\delta + qd)) \cap (\alpha) = (\beta).$$

Ist nun für irgendwelches z das Element $\gamma + c + z\omega$ in $\mathfrak{a}$ nicht enthalten, so gilt für das entsprechende Ideal $\mathfrak{b} \neq \mathfrak{a}$. Ist dagegen $\gamma + c + z\omega \in \mathfrak{a}$ für jedes z, so ist $\gamma + c \in \mathfrak{a}$, $\omega \in \mathfrak{a}$. Dabei gilt wegen (24) $(\delta + qd)\alpha = (\lambda + l)(\gamma + c)\alpha$ mit passenden λ, l, also

$$\delta + qd = (\lambda + l)(\gamma + c) + t\omega$$

mit irgendwelchem t. Da aber $\omega \in \mathfrak{a} \cap (\alpha) = ((\gamma + c)\alpha)$ ist, können wir $t = 0$ setzen. Dies bedeutet, daß $\mathfrak{a} = (\gamma + c)$ ist.

Es bleibt noch der Fall, wo $\mathfrak{o}=0$, d. h. α kein Nullteiler ist, übrig. Der Ring R^* mit den Verknüpfungen (17) ist auch in diesem Falle eine Schreiersche Erweiterung von R mit Einselement. Das Element α ist in R^* auch kein Nullteiler, denn aus $(\varrho+r)\alpha=0$ folgt $r\alpha=-\varrho\alpha\in(\alpha^2)$, also $r=0$ und damit $\varrho\alpha=0$, also $\varrho=0$. Ist nun $\mathfrak{a}$ ein Ideal in R^*, so sei $\mathfrak{a}(\alpha)=((\beta+b)\alpha)$. Für $\lambda+l\in\mathfrak{a}$ gilt dann

$$(\lambda+l)\alpha=(\xi+x)(\beta+b)\alpha,$$

also wegen der Regularität von α auch $\lambda+l=(\xi+x)(\beta+b)$, d. h. $\mathfrak{a}\subseteq(\beta+b)$. Andererseits, wenn $\gamma_1+c_1, \gamma_2+c_2, \ldots$ ein Erzeugendensystem von $\mathfrak{a}$ ist, so gilt für ein passendes m

$$(\beta+b)\alpha=(\xi_1+x_1)(\gamma_1+c_1)\alpha+\cdots+(\xi_m+x_m)(\gamma_m+c_m)\alpha,$$

also auch

$$\beta+b=(\xi_1+x_1)(\gamma_1+c_1)+\cdots+(\xi_m+x_m)(\gamma_m+c_m),$$

d. h. $\beta+b\in\mathfrak{a}$ und damit $\mathfrak{a}=(\beta+b)$. Hiermit ist Satz 4 bewiesen.

Es ist leicht zu sehen, daß auch umgekehrt, falls R ein k. H. E. und (α) ein Ideal in R ist, und zwar so, daß $R/(\alpha)\cong I/(n)$ mit einer natürlichen Zahl n gilt, dann (α) selbst ein Hauptidealring ist. Damit können wir die erhaltenen Ergebnisse folgenderweise zusammenfassen:

Jeder kommutative Hauptidealring R zerfällt in eine direkte Summe $R=R_1\dotplus R_2$, wobei $R_1=0$ oder R_1 ein k. H. E. ist und für R_2 einer der folgenden drei Fälle besteht:

$$1.\ R_2=0, \qquad 2.\ R_2\cong N, \qquad 3.\ R_2=R_{21}\dotplus\cdots\dotplus R_{2n},$$

wo jeder R_{2i} ein Ideal in einem u. H. E. R_{2i}^* ist und $R_{2i}^*/R_{2i}\cong I/(n_i)$ mit einer natürlichen Zahl n_i gilt, wobei $(n_i, n_j)=1$ für $i\neq j$.

Es ist nicht schwer zu zeigen, daß eine so erhaltene direkte Zerlegung eines beliebigen kommutativen Hauptidealringes in eine direkte Summe von unzerlegbaren Hauptidealringen (bis auf Ordnung der Summanden) eindeutig ist.

Literatur

[1] B. Brown—N. H. McCoy, Rings with unit element which contain a given ring, *Duke Math. J.*, **13** (1946), 9—20.

(Eingegangen am 26. April 1960)